

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Daniel Yon, a Special Agent with Homeland Security Investigations, being duly sworn, depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent (“SA”) of U.S. Department of Homeland Security, Homeland Security Investigations (“HSI”), since 2011, and am currently assigned to the Resident Agent in Charge, Springfield, Massachusetts office. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center (FLETC) and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media.

2. In addition, I have received specialized training and experience in the area of computer forensics and digital evidence recovery while attending Basic Computer Evidence Recovery Training (BCERT) at FLETC and Advanced Computer Evidence Recovery Training at the Computer Crimes Center in Fairfax, Virginia. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

3. This Affidavit is submitted in support of a criminal complaint charging Benjamin SHACAR with receipt and possession and access with intent to view child pornography in violation of 18 U.S.C. §§ 2252A(a)(2), 2252A(a)(5)(B).

4. The statements contained in this affidavit are based in part on information provided by U.S. federal law enforcement agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, including foreign law enforcement agencies, information gathered from the service of administrative subpoenas; the results of surveillance conducted by law enforcement agents; independent investigation and analysis by law enforcement agents/analysts and computer forensic professionals; and my experience, training and background as a Special Agent. Since this Affidavit is being submitted for the limited purpose of securing a criminal complaint.

STATUTORY AUTHORITY

5. 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) prohibit a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

6. 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

7. The following definitions apply to this Affidavit:

a. “Bulletin Board” means an Internet-based website that is either secured (accessible with a password) or unsecured, and provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as “internet forums” or “message boards.” A “post” or “posting” is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message “thread,” often labeled a “topic,” refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide the ability for members to communicate on a one-to-one basis through “private messages.” Private messages are similar to e-mail messages that are sent between two members of a bulletin board. They are accessible only by the users who sent/received such a message, or by the bulletin board administrator.

b. “Chat,” as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

c. “Chat room,” as used herein, refers to the ability of individuals to meet in one location on the Internet in order to communicate electronically in real-time to other individuals.

Individuals may also have the ability to transmit electronic files to other individuals within the chat room.

d. “Child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

e. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

f. “Cloud storage,” as used herein, is a form of digital data storage in which the digital data is stored on remote servers hosted by a third party (as opposed to, for example, on a user’s computer or other local storage device) and is made available to users over a network, typically the Internet.

g. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

h. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, “thumb,” “jump,” or “flash” drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

i. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

j. The “Domain Name System” or “DNS” is system that translates readable Internet domain names such as www.justice.gov into the numerical IP addresses of the computer server that hosts the website.

k. “Encryption” is the process of converting data into a code in order to prevent unauthorized access to the data.

l. A “hidden service,” also known as an “onion service,” is website or other web service that is accessible only to users operating within the Tor anonymity network.

m. “Hyperlink” refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

n. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

o. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

p. An “Internet Protocol address” or “IP address,” as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (“ISPs”) control a range of IP addresses. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be “static,” if an

ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

q. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

r. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

s. "Remote computing service," as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

t. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

u. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

v. The "Tor network" is a computer network available to Internet users that is designed specifically to facilitate anonymous communication over the Internet. The Tor network

attempts to do this by routing Tor user communications through a globally distributed network of relay computers, along a randomly assigned path known as a “circuit.”

w. “URL” is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

x. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

y. A “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

8. A user (later determined to be SHACAR) of the Internet account at the SUBJECT PREMISES (18 Maple Street, Pittsfield, MA) has been linked to an online community of individuals who regularly send and receive child pornography via a hidden service website that operated on the Tor anonymity network. The website is described below and referred to herein

as the “TARGET WEBSITE.”¹ There is probable cause to believe that a user of the Internet account at the SUBJECT PREMISES accessed the TARGET WEBSITE, as further described herein. There is probable cause to believe that the user, SHACAR, at 18 Maple Street, accessed the TARGET WEBSITE.

The Tor Network

9. The Internet is a global network of computers and other devices. Devices directly connected to the Internet are uniquely identified by IP addresses, which are used to route information between Internet-connected devices. Generally, when one device requests information from a second device, the requesting device specifies its own IP address so that the responding device knows where to send its response. On the Internet, data transferred between devices is split into discrete packets, each of which has two parts: a header with non-content routing and control information, such as the packet’s source and destination IP addresses; and a payload, which generally contains user data or the content of a communication.

10. The website further described below operated on the Tor network, which is a computer network available to Internet users that is designed specifically to facilitate anonymous communication over the Internet. The Tor network attempts to do this by routing Tor user communications through a globally distributed network of relay computers, along a randomly assigned path known as a “circuit.” Because of the way the Tor network routes communications

¹ The name of the TARGET WEBSITE is known to law enforcement. Investigation into the users of the website remains ongoing and disclosure of the name of the website would potentially alert active website users to the investigation, potentially provoking users to notify other users of law enforcement action, flee, and/or destroy evidence.

through the relay computers, traditional IP address-based identification techniques are not effective.

11. To access the Tor network, a user must install Tor software. That is most easily done by downloading the free “Tor browser” from the Tor Project, the private entity that maintains the Tor network, via their website at www.torproject.org.² The Tor browser is a web browser that is configured to route a user’s Internet traffic through the Tor network.

12. As with other Internet communications, a Tor user’s communications are split into packets containing header information and a payload, and are routed using IP addresses. In order for a Tor user’s communications to be routed through the Tor network, a Tor user necessarily (and voluntarily) shares the user’s IP address with Tor network relay computers, which are called “nodes.” This routing information is stored in the header portion of the packet. As the packets travel through the Tor network, each node is able to see the address information of the previous node the communication came from and the next node the information should be sent to. Those Tor nodes are operated by volunteers – individuals or entities who have donated computers or computing power to the Tor network in order for it to operate.

13. Tor may be used to access open-Internet websites like www.justice.gov. Because a Tor user’s communications are routed through multiple nodes before reaching their destination, when a Tor user accesses such an Internet website, only the IP address of the last relay computer (the “exit node”), as opposed to the Tor user’s actual IP address, appears on that website’s IP address log. In addition, the content of a Tor user’s communications are encrypted while the

² Tor users may also choose to manually configure a web browser or other application to route communications through the Tor network.

communication passes through the Tor network. That can prevent the operator of a Tor node from observing the content (but not the routing information) of other Tor users' communications.

14. The Tor Project maintains a publicly available frequently asked questions (FAQ) page, accessible from its website, with information about the Tor network. Within those FAQ, the Tor Project advises Tor users that the first Tor relay to which a user connects can see the Tor user's actual IP address. In addition, the FAQ also cautions Tor users that the use of the Tor network does not render a user's communications totally anonymous. For example, in the Tor Project's FAQ, the question "So I'm totally anonymous if I use Tor?" is asked, to which the response is, in bold text, "No."

15. The Tor Network also makes it possible for users to operate or access websites that are accessible only to users operating within the Tor network. Such websites are called "hidden services" or "onion services." They operate in a manner that attempts to conceal the true IP address of the computer hosting the website. Like other websites, hidden services are hosted on computer servers that communicate through IP addresses. However, hidden services have unique technical features that attempt to conceal the computer server's location.

16. Unlike standard Internet websites, a Tor-based web address is comprised of a series of either 16 or 56 algorithm-generated characters, for example "asdlk8fs9dfiku7f," followed by the suffix ".onion." Ordinarily, investigators can determine the IP address of the computer server hosting a website (such as www.justice.gov) by simply looking it up on a publicly available Domain Name System ("DNS") listing. Unlike ordinary Internet websites, however, there is no publicly available DNS listing through which one can query the IP address of a computer server that hosts a Tor hidden service. So, while law enforcement agents can often

view and access hidden services that are facilitating illegal activity, they cannot determine the IP address of a Tor hidden service computer server via public lookups. Additionally, as with all Tor communications, communications between users' computers and a Tor hidden service webserver are routed through a series of intermediary computers. Accordingly, neither law enforcement nor hidden-service users can use public lookups or ordinary investigative means to determine the true IP address – and therefore the location – of a computer server that hosts a hidden service.

Description of TARGET WEBSITE

17. The TARGET WEBSITE was an online chat site whose primary purpose is to share and distribute child pornography. The advertisement and distribution of child pornography and child erotica were regular occurrences on this site. The TARGET WEBSITE started operating in approximately 2018 and appeared to cease operating in 2020.

18. The TARGET WEBSITE's front page stated that the site was intended for users to "post links with good photos and videos" depicting "[o]nly GIRLS 4 to 14 years [old]." The site allowed users to engage in online chat with other users, either within chat rooms that were openly accessible to any user of the site, within rooms only accessible to particular users, or in one-to-one chats between two users. Child pornography images and videos were trafficked through this chat site via the posting of web links within chat messages. Links allowed a user to navigate to another website, such as a file-hosting website, where images and/or videos were stored in order to download these image and videos. The TARGET WEBSITE provided its users with information about particular file hosting websites where users could upload digital files so that the files could then be shared, via links, with other users on the TARGET WEBSITE.

19. Entry to the site is obtained through free registration, as described below. On the registration page, it reads, among other things, “No hurtcore, No gore, No zoo, No death, No toddlers.” In my training and experience, “zoo” refers to pornography depicting bestiality, and “hurtcore” is a genre of child pornography that depicts violence, gore, torture, humiliation, or children in pain and distress. In addition, the registration page of the TARGET WEBSITE expressly contemplated the sharing of videos between members. Language on that page reads “Post links with good photos and videos (preview is required!).”

20. In order to pass through the registration page and gain access to the actual content of the TARGET WEBSITE, a prospective user must create a “Nickname” and a password which must be entered along with a Captcha. A “Captcha” is a randomly generated series of characters designed to ensure that users of a website are human beings and not bots or other automated processes. Users are not required to enter any personally identifiable information, such as true names, emails or phone numbers. The users may also pick a color for their posts (or one was randomly generated) and click “enter chat.”

21. Upon initially creating a user account on the TARGET WEBSITE, a user was assigned the status of “Guest.” As an unregistered user, the user receives the following message upon log in: “As it looks like you are not registered you may check our rules by sending to me word rules. There also will be some additional explanation of how to use this feature. News! We added feature of forum. Access by button at the bottom or just by this link: forum. this should make you be more happy of getting this message on entrance.” Unregistered or “Guest” users could access TARGET WEBSITE postings including postings that shared child pornography images.

22. In order to fully register an account, the user would need to obtain a promotion from “Guest” to “Registered Guest,” which is done at the discretion of TARGET WEBSITE staff. After an individual is promoted to a registered user account on the TARGET WEBSITE, a user must log in to that user account with the appropriate user-generated password in order to communicate via that user account on the TARGET WEBSITE. TARGET WEBSITE users may register, log into and access the TARGET WEBSITE through that user account using any computer or electronic device that is configured to use Tor routing/software.

23. As is common on these types of sites, the TARGET WEBSITE was administered and moderated by select TARGET WEBSITE users referred to as “Members” on this site. These users are promoted at the discretion of the site leadership. Promotions appeared to be made based on an individual’s active participation on the site. Once promoted to a Member position, those users enforced the rules and assisted in the management of the site. This included controlling user membership using the “ban” and “kick” functions (which can limit or eliminate a user’s participation or account), promoting within the ranks of users, and moderating the public chatroom for content and user behavior.

24. TARGET WEBSITE Members periodically re-posted standard messages to the public chatroom of the TARGET WEBSITE iterating rules and procedures of the TARGET WEBSITE. For example, on or about May 28, 2019, a Member on the TARGET WEBSITE posted “CHAT RULES” in the public chatroom. This post contained statements in both Russian and English which included but was not limited to, “Follow the requests of the Members,” “No hurtcore, No gore, No zoo, No death, No toddler,” “Only GIRLS 5 to 13 years. Any language allowed,” and “For RG (registered guests) the photo archive is available (the “links” button).”

25. In addition, postings to the TARGET WEBSITE that were publicly available to any registered user of the TARGET WEBSITE were captured and archived for law enforcement review. Review of such postings disclosed the following posts by TARGET WEBSITE users:

An image file titled “MATRIX_235841_tEu_004.jpg”, which depicts a female child approximately 8-10 years of age laying on a red, green, white, and blue plaid colored blanket. The child appears to be the same child as described in the images titled; 1549037966.jpg and 1556381394.jpg. The blanket appears to be on a large bed as the wood headboard and nightstand are visible in the photograph. The child is completely nude laying on her back with knees bent and legs spread revealing her genitalia as the central focal point of the image.

An image file titled “1549037966.jpg”, which depicts a female child approximately 8-10 years of age laying on a red, green, white, and blue plaid colored blanket. The child appears to be the same child as described in the images titled; MATRIX_235841_tEu_004.jpg and 1556381394.jpg. The child is depicted nude from the waist down wearing only a shirt. She is laying on her back with knees bent and legs spread revealing her genitalia as the central focal point of the image.

An image file titled “1556381394.jpg”, which depicts a female child approximately 8-10 years of age laying on a red, green, white, and blue plaid colored blanket. The child appears to be the same child as described in the images titled; 1549037966.jpg and MATRIX_235841_tEu_004.jpg. The child is depicted completely nude with her arms crossed and legs spread. There is an adult male depicted in the foreground of the image who also appears to be completely nude. The man is seen penetrating the child vaginally

with an erect penis. The image is depicted from the viewpoint of the adult male with the sexual act as focal point of the image.

Evidence Related to Identification of Target that Accessed TARGET WEBSITE

26. My agency was provided with reliable information that a user had accessed the TARGET WEBSITE. Specifically, my agency learned that on May 2, 2019, IP address 24.194.90.108 accessed the TARGET WEBSITE.

27. As described herein, the TARGET WEBSITE could not generally be accessed through the traditional internet. Only a user who had installed the appropriate Tor software on the user's computer could access the "TARGET WEBSITE." Even after connecting to the Tor network, however, a user would have to find the 16-or-56-character web address of the TARGET WEBSITE in order to access it. Hidden service websites on the Tor Network are not "indexed" by search engines—such as Google—to anywhere near the same degree as websites that operate on the open Internet. Accordingly, it is much more difficult to perform a Google-type search of hidden service websites than it is to search open Internet websites for particular content of interest. Users interested in accessing child exploitation material (or in advertising child exploitation and pornography websites they operate) therefore keep, maintain and use directory sites that advertise the web addresses of hidden services that contain child exploitation related content. Those directory sites also operate via the Tor network. Users utilize those directory sites to identify new web forums, chat sites, image galleries and file hosts pertaining to the sexual exploitation of children. Such directory sites often identify whether particular sites are then operating, whether child pornography imagery may be found there, and even what types of child pornography are accessible (i.e., boys, girls, or "hurtcore"). They also contain clickable

hyperlinks to access those sites. As with other hidden service websites, a user must find the 16-or-56 character web address for a directory website in order to access it. While it operated, the web address for the website described herein was listed on one or more of such directory sites advertising hidden services dedicated to the sexual exploitation of children.

28. I am also aware through consultation with FBI agents that the review of detailed user data related to one Tor network based child pornography website found that it was exceedingly rare for a registered website user to access that website and never return. FBI review of user data from that website found that less than two hundredths of one percent of user accounts registered an account on the website, accessed a message thread on the website, and then never returned to the website and logged in to the same account.

29. Accordingly, based on my training and experience and the information articulated herein, because accessing the TARGET WEBSITE required numerous affirmative steps by the user – to include downloading Tor software, accessing the Tor network, finding the web address for TARGET WEBSITE, and then connecting to TARGET WEBSITE via Tor – it is extremely unlikely that any user could simply stumble upon TARGET WEBSITE without understanding its purpose and content.

30. Accordingly, I submit that there is probable cause to believe that, for all of the reasons described herein, any user who accessed the TARGET WEBSITE has, at a minimum, knowingly accessed the TARGET WEBSITE with intent to view child pornography, or attempted to do so.

Identification of 18 Maple Street, Pittsfield, MA

31. According to publicly available information, IP address 24.194.90.108, which was used to access TARGET WEBSITE on May 2, 2019 was registered to Charter Communications, Inc.

32. On March 18, 2020, a subpoena/summons was issued to Charter Communications, in regard to the pertinent IP address. A review of the results obtained on March 21, 2020, identified the following account holder and address, which is the address of the SUBJECT PREMISES:

Subscriber Name: Benjamin Shacar
Subscriber Address: 18 Maple St, Pittsfield, MA 01201-4813
User Name or Features: broken.poet@gmail.com
Phone Number: (413)358-0101
Account Number: 379189815

33. A search of a public records database that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, and other information was conducted for Benjamin SHACAR. These public records indicated that SHACAR's current address is 18 Maple St, Pittsfield, MA 01201.

34. A check with the Massachusetts Registry of Motor Vehicles (RMV) on or about January 7, 2021 revealed that the subject Benjamin Michael SHACAR, resides at the SUBJECT PREMISES. Additional RMV records list a 2012 white Jeep Liberty bearing Massachusetts license plate 9MHW40 registered to SHACAR at the SUBJECT PREMISES, and a 2014 grey Honda Odyssey bearing Massachusetts license plate 2GDM61 co-owned with his wife, Desiree SHACAR registered to both subjects at the SUBJECT PREMISES.

35. On December 10, 2020, at approximately 2:19 PM, a white Jeep Liberty matching the description of the vehicle registered to SHACAR and a grey Honda Odyssey matching the description of the vehicle co-owned by Benjamin and Desiree SHACAR was observed at the SUBJECT PREMISES.

36. On January 14, 2021, a vehicle matching the description of the 2014 grey Honda Odyssey registered to Benjamin and Desiree SHACAR was overserved parked in the driveway of the SUBJECT PREMISES.

37. On January 15, 2021, representatives of Eversource Energy indicated that service is being provided to the tenant Benjamin M. SHACAR at the SUBJECT PREMISES.

38. On January 15, 2021, a check with United States Postal Service (USPS) revealed the last name SHACAR as receiving first class mail service at the SUBJECT PREMISES.

39. A check of open source information from the Internet regarding Benjamin SHACAR revealed a Facebook page for Benjamin M Shacar which publicly displays a profile picture depicting a male and female together. The male depicted in the image matches Benjamin SHACAR's RMV photograph and the female matches Desiree SHACAR's RMV photograph. Located under the About, Family and Relationships section, SHACAR's Relationship is listed as "Married to Dzray Chezcar since March 1, 2014" with a link to a Facebook page for an individual with the display name Dzray Chezcar (Desiree).

40. On the separate Facebook page for Dzray Chezcar (Desiree), located on the main page under the "Intro" section the page states, "Pronounces name DES-err-ay SHAY-karr". The website publicly displays a photograph of female matching Desiree SHACAR's RMV photograph. Another publicly displayed photograph shows Desiree SHACAR holding a young

child outdoors, near a house matching the description of 14 Maple Street, as well as the SUBJECT PREMISES. The image depicts a house with grey shingle siding and green trim consistent with that of 14 Maple Street and another with white and a light yellow siding consistent with that of the SUBJECT PREMISES.

41. The photo has a comment from an individual linked to a Facebook page for Carlos Shacar. The comment reads, “So beutifull love you dearly!!!”. The person operating the Dzray Chezcar page responded to the comment by posting an image stating, “Thanks Dad” and another image stating, “love you, dad”.

42. According to law enforcement records checks, Benjamin SHACAR (formerly known as Benjamin ERRICHETTO) has a juvenile criminal history including six counts of indecent assault and battery on a child under the age of fourteen. He was arraigned on January 8, 2001 at the age of thirteen in the Berkshire County Juvenile Court. According to the record, a Jury Trial on May 14, 2001 appears to have moved the case to the Pittsfield Juvenile Court, where it was continued without a finding. A violation notice was then sent on June 10, 2002, and the case was then continued on June 25, 2002. The last date of action in the record indicates that the charges were ultimately dismissed on June 20, 2005. According to management at the Pittsfield Juvenile Court, this type of incident is common practice for juveniles that do not reoffend within a certain timeframe.

43. On March 24, 2021, I, along with other law enforcement agents, executed a federal search warrant for 18 Maple Street, Pittsfield, MA, the top floor of the two-story structure that is 16-18 Maple Street.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

44. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as “WiFi” or “Bluetooth.” Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer’s ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various

types - to include computer hard drives, external hard drives, CDs, DVDs, and “thumb,” “jump,” or “flash” drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual’s person. Smartphones and/or mobile phones are also often carried on an individual’s person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as “cloud” storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user’s computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as “apps.” Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or

playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

h. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that mobile device users often connect to known wireless networks which are available to them, especially localized networks within their residence. The connection information such as usernames and passwords are typically stored within the device and the device automatically connects when within range of a known wireless network. Individuals often set this automatic connect preference in their devices in order to conserve battery consumption, improve connection speeds, and reduce cellular data consumption which is often limited or metered. Mobile devices connected to a wireless network will often share the same IP address information as reported by the residential wireless network provider.

i. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a

computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO ACCESS WITH INTENT TO VIEW, POSSESS AND/OR RECEIVE CHILD PORNOGRAPHY

45. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who access online child sexual abuse and exploitation material via a website:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain child pornographic material in the privacy and security of their home or some other secure location.

Individuals who have a sexual interest in children or images of children typically retain those materials and child erotica for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.³

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit

³ See *United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); see also *United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370-71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)).

material, and often maintain contact information (e.g. online messaging accounts, email addresses, etc.) of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

h. Even if the target uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in his home, the SUBJECT PREMISES, as well as in (a) vehicle(s) located at the SUBJECT PREMISES, as set forth in Attachment A, including on digital devices other than the portable device (for reasons including the frequency of “backing up” or “synching” mobile phones to computers or other digital devices).

46. Based on all of the information contained herein, an internet user, later identified as SHACAR, residing at 18 Maple Street, Pittsfield, MA, displays characteristics common to individuals who access online child sexual abuse and exploitation material via a website. In particular, SHACAR obtained and used Tor network software, found the web address for TARGET WEBSITE, and accessed online child sexual abuse and exploitation material via the TARGET WEBSITE. Based on the characteristics common to individuals who access online child sexual abuse and exploitation material, as described herein, the internet user residing at 18 Maple Street that accessed the TARGET WEBSITE, later identified as SHACAR, also downloaded and maintained child sexual abuse and exploitation material from the TARGET WEBSITE and/or other online sources.

EXECUTION OF SEARCH WARRANT AT 18 MAPLE STREET

47. On March 22, 2021, I submitted an affidavit in support of a search warrant for 18 Maple Street based on the foregoing and other information to the U.S. Magistrate Judge in Springfield, MA. On that same day, the U.S. Magistrate Judge issued a search warrant for 18 Maple Street.

48. On the morning of March 24, 2021, I, along with a team of agents, executed the search warrant at 18 Maple Street, the SUBJECT PREMISES. Inside the two-story structure designated as 16-18 Maple Street (with 16 Maple Street being the ground floor and 18 Maple Street being the second floor) were SHACAR, Desiree Shacar, and three children. The second-floor unit, 18 Maple Street, was where SHACAR and his wife stayed, and this unit was searched. The first-floor unit, 16 Maple Street, was where the children stayed, and this unit was not searched.

49. The team and I (hereinafter the "Team") found several electronic devices at the SUBJECT PREMISES. At this time, the review of these items has been limited, due to the short amount of time between the execution of the search warrant and the writing of this affidavit. At the residence, SHACAR gave an interview after having been advised of his Miranda rights and choosing to waive them.

50. SHACAR identified a desktop computer as belonging to him, and he distinguished that desktop computer from another desktop computer belonging to his wife. A Tor browser was found on SHACAR's desktop computer. Also found was a laptop computer. SHACAR, after initially being reluctant to acknowledge his involvement in the receipt of child pornography, SHACAR admitted that he downloaded child pornography from the internet.

SHACAR indicated that he used the laptop computer for most of his child pornography activity. SHACAR also indicated that his desktop and laptop computers were unlikely to contain child pornography because he would either access child pornography sites and view child pornography without downloading it, or SHACAR would download it and transfer the child pornography to a thumb drive.

51. SHACAR identified where the thumb drive could be found—on top of a kitchen cabinet. He said he hid the thumb drive so no one would find it.

52. The thumb drive was previewed and it was found to contain approximately 80 child pornography videos, which tended to have descriptive files names that made it clear that the files were child pornography. My team was able to determine that approximately 10 videos depicted children who had been previously identified in other child exploitation investigations. Three such videos have the following file names and descriptions:

- a. 2016-01 Estefy - Opva Pthc 2015 11Yo And Uncle Best Anal Fuck Creampie
Ever!!!!_xvid.avi – This is video file is 11 minutes and 59 seconds in length. The video shows a prepubescent minor female perform oral sex on an adult male. Later in the video, the adult male touches the minor female's vagina and anus and spits into the minor female's vagina. The adult male then performs anal sex on the minor female.
- b. (PHANT)(pthc)(otstoi)(toddler suck) 7Yo and papa.mp4 - This is video file is 59 seconds in length. The video shows a prepubescent minor female wearing orange underwear pull down the pants of an adult male to expose an erect penis and the minor female performs oral sex on the adult male.
- c. (Pthc) 4Yo Pae (Great New Cbaby).!!New Dark Studio 10 cd1 (Dad and babyj) 3yo in

pink gives BJ.mpg - This is video file is 4 minutes and 20 seconds in length. The video shows a prepubescent minor female perform oral sex on an adult male. Later in the video, the naked minor female lays on her back and her vagina is visible. The minor female then masturbates the erect penis until the conclusion of the video.

53. SHACAR's laptop also had the Tor browser, which included a bookmark for a dark web site that SHACAR identified as being his favorite child pornography site. As indicated above, a Tor browser allows a user to access the "dark web" of unindexed sites on the internet, including the TARGET WEBSITE.

54. SHACAR said he accessed child pornography for his sexual gratification and that he had done so for many years. He said he had been accessing dark web sites since 2016. Prior to that, SHACAR said he used peer-to-peer (P2P) software to access and obtain child pornography from the internet. He said these P2P child pornography files tended to be infected with viruses and that this had caused problems for him.

55. SHACAR's wife was interviewed, and she indicated that she had no knowledge of any child pornography activities. Her desktop computer was previewed, and when no contraband was found, it was not taken.

CONCLUSION

56. Based on the foregoing, there is probable cause to believe that BENJAMIN

SHACAR committed the offenses of Receipt and Possession of Child Pornography.

Daniel R. Yon
Special Agent
Homeland Security Investigations

Sworn and subscribed before me this ____th day of _____, 2021.

Katherine A. Robertson
UNITED STATES MAGISTRATE JUDGE